12-3-2012

Secure Key Deployment and Exchange Protocol for Manet Information Management

Brian Cusack
Edith Cowan University

Alastair Nisbet
AUT University

Recommended Citation

Cusack, B., & Nisbet, A. (2012). Secure Key Deployment and Exchange Protocol for Manet Information Management. DOI: https://doi.org/10.4225/75/57b3adaafb85e

DOI: 10.4225/75/57b3adaafb85e
10th Australian Digital Forensics Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012

SECURE KEY DEPLOYMENT AND EXCHANGE PROTOCOL FOR MANET INFORMATION MANAGEMENT

Brian Cusack[1] and Alastair Nisbet
AUT UniversityAuckland, New Zealand
[1] SRI - Security Research Institute, Edith Cowan University, Perth, Western Australia
brian.cusack@aut.ac.nz; anisbet@aut.ac.nz

Abstract

Secure Key Deployment and Exchange Protocol (SKYE) is an innovative encryption Key Management Scheme (KMS) based on a combination of features from recent protocols combined with new features for Mobile Ad Hoc Networks (MANETs). The design focuses on a truly ad hoc networking environment where geographical size of the network, numbers of network members and mobility of the members is all unknown before deployment. This paper describes the process of development of the protocol and the application to system design to assure information security and potential evidential retention for forensic purposes. Threshold encryption key management is utilized and simulation results show that security within the network can be increased by requiring more servers to collaborate to produce a certificate for a new member, or by requiring a higher trust threshold along the certificate request chain. The cost of information management (eg. time, processor use and battery use in mobile devices) is also a consideration.

Keywords
Security, Information Management, Wireless, Networks, MANET, Simulation

INTRODUCTION

Ad Hoc networks are distinguished from infrastructure networks in that the network members, or nodes, communicate directly with each other rather than through a fixed access point. They differ from a mesh network in that a truly ad hoc network is created 'on the fly' for a specific, sometimes spontaneous purpose, and is often disbanded soon after its usefulness has ended. Whilst a mesh network may consist of many stationary nodes, an ad hoc network will often be dynamic, with nodes frequently joining or leaving the network and with some nodes mobile throughout the network. It is this very dynamic nature of the type of network that creates such difficulties in implementing robust security (Capkun, Buttyan and Hubaux, 2003). Similarly the open nature of such networks raises issues of malicious agents and the problem of retaining information for post event investigation. Security implies control, whether it be by physical control of the network or control by some member or members who have authority to manage access. However, truly ad hoc networks present significant challenges in instigating security because of their very open nature and lack of a controlling entity.

Security for MANETs includes five attributes: availability, authentication, confidentiality, integrity and non-repudiation. In an ad hoc environment, to achieve these five attributes firstly requires that any member of the network must be able to be identified (Frankel, Eydt, Owens, and Scarefone, 2007). This is vital if malicious members are to be identified and permanently ejected from the network. A non-changeable identity can be linked to some unique physical attribute of the device such as the CPU serial number, meaning once that attribute is recorded, the node's behaviour can be monitored and if necessary the node's permission to join the network can be revoked. Additionally, robust encryption of the data is needed to prevent nodes reading messages intended only for an authorized recipient (Chen, Yao and Wang, 2010). This is critical because of the security and information retention constraints in wireless communications. Generally, wireless devices transmit their messages omnidirectionally, meaning other similar devices within radio range can read the message. With radio ranges of at least several hundred metres for most wireless standards, preventing messages reaching unintended recipients is almost impossible. Therefore, encryption is the best method for protecting the message from these unauthorized nodes. Whilst the data may be captured by unauthorized nodes, without the appropriate decryption key the message will remain unreadable and therefore secure. To encrypt and decrypt messages in a network, encryption keys must be created, distributed and when necessary revoked (Gennaro, Jarecki, Krawczyk, and Rabin, T., 2007). Whilst several protocols have been proposed for these types of networks, the important aspects of the design that are open for improvement is both effectiveness and efficiency. Effectiveness can be measured by how well the protocol achieves its goal. The main goal is to create and distribute certificates to requesting nodes as they wish to join the network. Therefore, the success rate of the requests is a good measure. For efficiency, the measure is how the network performs as security is increased. Inevitably higher security will lead to a reduced success rate for certificate requests, and it is the impact on increasing security that can be used as a

measure of efficiency. Similarly evidential retention of successful and unsuccessful requests, and records of agent behaviour can be used as measures for forensic readiness.

This paper is structured to first define the SKYE protocol and then to scenario test it utilizing simulation. The discussion of results shows that this protocol performs effectively and efficiently within a large number of scenarios. The tuneable nature of the protocol allows settings to be adjusted so that efficiency can be compromised to allow higher security where necessary. Additionally, forensic evidence can be incorporated into the protocol so that the considerable complications of key recovery caused by threshold cryptography can still permit recovery of evidence whilst retaining high security (Zhou, and Haas, 1999; Wu, Wu, Fernandez, Ilyas, and Magliveras, 2005).

THE SKYE PROTOCOL

There are two distinct encryption methods: symmetric key encryption where the same key is used for encryption and decryption, and asymmetric encryption where a public key is freely given out and is used to encrypt a message and a private key known only to the recipient is used to decrypt the message (Yi, and Kravets, 2004). Symmetric encryption is less computationally draining (ie. battery power), but for total privacy of data it requires nodes to share the same secret key. This key creation and exchange can be done securely before network deployment or can be performed dynamically as required. Asymmetric encryption is robust, but requires the use of a Certificate Authority (CA) often called a Trusted Third Party, to create and distribute certificates validating the identities and the keys bound to those identities. Finding an efficient way to create and maintain an easily contactable CA is very challenging, especially when nodes in the network are mobile (Hyytiä, and Virtamo, 2007). However, with a truly ad hoc network where members have no prior knowledge or prior contact with each other, implementing control over the network is extremely difficult. The challenge in this area is to allow a highly dynamic network formation where all security is implemented after network formation. One consideration when designing a protocol is that it must be practical so that there is a balance between features of the design and the efficiency. Generally, as security is increased the complexity of the protocol also increases. More complexity will mean higher battery drain of the devices and more latency in performing the key management tasks. A very secure protocol may simply be unworkable in practice, and a very basic protocol may be so insecure as to be unusable. The goal of this protocol is to provide a key management scheme suitable for a truly ad hoc network with a high number of members with large geographical size. Any node can join the network meaning malicious nodes will inevitably become members. To counter this, monitoring of agent behaviour is required along with planning for evidential retention (Kong, Zerfos, Luo, Lu, and Zhang, 2001).

The process for the design of SKYE was to thoroughly review the previous relevant protocols and note any that showed promise for this type of network. The many previously designed protocols were reduced to a few, and their positive attributes noted. Any negative attributes were noted in an effort to avoid any features that may be detrimental. Additionally, possible uses for the protocol were also identified. Whilst the uses may include military, educational, public and any other use involving a rapid deployment of a network, one possible application stood out (Kurkowski, Camp, and Colagrosso, 2005). This is disaster relief and recovery where disaster victims may be able to establish a network for communications where other communication infrastructure has failed. If there is a large area affected by some natural disaster with all communications disabled, then people inside the disaster area could form an ad hoc network using computers, WiFi equipped cellphones or PDAs and begin communicating with neighbours. As the networks grow, pockets of smaller networks join with other networks to eventually form a large network where every node can connect to every other node using intermediate nodes to pass on messages. When help arrives in the form of rescue workers, they can join the established network and immediately send and receive vital information about the disaster area and the victims. Additionally, outside communication may be possible so long as at least one node in the network is connected to the outside world, possibly through the Internet. Even in this type of scenario, security is vital for several reasons. Firstly, some messages may be highly confidential and must remain private from all but the intended recipient. Secondly, if any node can join the network but never be excluded, a misbehaving node could seriously upset the running of the network by excessive message sending, failing to pass on messages or sending false messages. It is desirable then to have a protocol in place that can efficiently provide evidential retention and all three key management functions: key creation, key exchange and key revocation; along with network logging of key management tasks(Zimmerman,1994; Johnson, and Maltz, 1996; Zhu, Bao, Deng, Kankanhalli and Wang, 2005).

By looking at the type of scenario the protocol may be used for, the following desirable characteristics are identified and relevant protocol features defined in Table 1.

Attribute	Definition
Any node should be able to join the network. No prior knowledge or offline configuration should be necessary.	The combination of not having any offline configuration but using digital certificates to bind keys to identities leads to self certification of nodes or servers issuing certificates to nodes. Using threshold cryptography and a certificate authority requires a choice of how many servers should be required before a certificate can be issued. This assumes that the network begins with 100 nodes or so as any less would mean that not enough servers are available to provide certificate services. With the network beginning with a single node and growing dynamically, the current protocol utilises a minimum server's required threshold but overrides that rule until enough servers are present to meet the threshold.
Key management messages should be the least number possible to provide the service. The number of messages utilises more bandwidth than the size of the messages, so larger messages but less of them is desirable. Additionally, a choice of encryption should be available to save battery power where possible.	From a security standpoint, some messages do not require high security, or perhaps any security. Encryption and decryption calculations require considerable CPU usage. For messages that require little or no privacy, it is therefore desirable to send them unencrypted or with lower encryption saving valuable battery power. This leads to the desirable functionality of ranking messages with a corresponding security level and using the appropriate encryption for the level. There should be three levels of security for messages similar to that used for military communications. That is, unclassified where no encryption is used, classified using symmetric encryption and secret utilising PKI.
Keys should only be exchanged with nodes that the sender needs to communicate with.	Exchanging keys with only those nodes that it is necessary for communication saves considerable key management overhead. The sender first selects the security level, open, symmetric or asymmetric encryption. The process is then: a. Sender checks with closest server that the receiver has a valid certificate. b. Server first checks sender's certificate and then replies with confirmation of receiver's certificate. c. Sender requests communication with receiver and sends his certificate details and symmetric key if level 2 security is selected. d. Receiver checks with closest server that the sender has a valid certificate. e. Server first checks receiver's certificate and then replies with confirmation of sender's certificate. f. Receiver replies to sender and communication begins.
All nodes should be able to communicate with all other authorised nodes in the network.	Provided the communicating nodes are part of the same network, the routing protocol employed should ensure that contact can be made between the two nodes. Only nodes holding valid certificates can exchange messages, but nodes that have not yet been issued certificates can pass on certificate issuance requests. If this were not permitted, no requests could ever be forwarded to a server.
Certificates binding keys to nodes identities should be used for high security.	The use of digital certificates binding keys to the node's identity raises two points. Firstly, the identity of the node must positively identify it and must not be able to be changed or spoofed. To ensure robustness against attack, redundancy, which provides fault tolerance and high availability, a distributed CA using threshold cryptography is employed. The CA will comprise of k nodes out of n nodes in the network. A subset of the k nodes must combine to provide CA services.
If a node misbehaves, it should be identified and if necessary permanently excluded from the network.	To eject a node from the network, misbehaviour must be identified and noted. Neighbouring nodes are responsible for monitoring each other's behaviour. Each node joins the network with total trust. The trust is measured from full trust of 1 to very low trust of 0.1. Each instance of

	malicious behaviour identified reduces the trust in that node from the accuser of 0.1. The trust level is used when a node requests a certificate. The trust level along the certificate chain is calculated along with the attenuation factor (0.1 for every hop along the chain) and this final calculation is used by a server to decide whether a certificate should be issued or not.
A single node should not have the power to eject another node.	A threshold of accusations is required to eject a node ensuring that no single node can maliciously eject any other node.
An excluded node should still receive vital information	Any messages deemed unclassified such as messages about rescue efforts or warnings of impending danger in a disaster situation are sent unencrypted and can be read by all nodes, including those ejected or those who are not currently authenticated.
The network should be highly scalable.	For a network to be highly scalable, nodes must be able to communicate at the same time without interfering with others communication. With a maximum radio range of approximately 300 metres it is envisaged that with a widely dispersed network only limited numbers of nodes will be within range of each other. The scalability of the network therefore uses the limited radio range of the devices along with the key exchange on a demand basis to assist with scalability.
The network should handle mobility of nodes efficiently.	Mobility of the nodes should present no problems with the key management as key exchange is on a demand basis and network wide protocols are employed where geographic relocation of the nodes will make no difference to the keys employed providing the node remains within the same network. Additionally, the CA will be dispersed and the same number of CA servers will need to be contacted for certificate servers wherever the node may be. Therefore, mobility of the nodes will effectively be transparent to the members of the network, including the CA servers.

Table 1: MANET desirable attributes

SIMULATIONS

A suitable wireless simulator was sought and several simulators investigated. None proved suitable with the considerable customisation required and eventually Matlab was chosen as the basis for constructing a custom built simulator. Each simulation scenario was run several times and the results averaged for each run. A node mobility of 20% of nodes was selected as a realistic baseline with each node having an equal chance of being mobile. The mobile nodes chose a random speed between 20-29kmh and Random Waypoint Mobility was used as the mobility model. The simulation begins with one randomly placed node on a 2.5km x 2.5km area, growing and shrinking dynamically with 30 nodes per minute randomly added and 10 nodes per minute randomly leaving. Table 2 shows the fixed parameters used for the simulation runs.

Simulation area (metres square)	2500
Simulation time (seconds)	600
Nodes present at start	1
Node growth per minute (Poisson distribution)	30
Node leave per minute (Poisson distribution)	10
Node mobility model	RWPM
Node pause time (seconds)	0-10
Nodes malicious (percent)	6%
Malicious message threshold	3
Accusation ejection threshold	5
Accusation ejection timeout (seconds)	60
Simulation runs averaged	10
Communication distance (metres)	300
Private message exchange rate / sec	0.1

Table 2: Simulation fixed parameters

A malicious node threshold of 6% of the nodes was chosen based on NZ crime statistics (NZ Police, 2004). This figure is deliberately low as malicious behaviour is predicted to be rare in the likely scenarios. For example, an educational setting could expect little or no malicious behaviour, but military use in a hostile environment may see many attempts at attacking the network. For the purpose of the simulation, malicious behaviour involves nodes failing to pass on every third message. This resulted in the trust in that node from the previous node being reduced by 0.1. The node would then make an accusation against the malicious node to one of the servers. If 5 accusations were received within 60 seconds, the malicious node was permanently ejected from the network. With a radio communication range of 300 metres to mimic IEEE 802.11b,g and n and nodes placed at random, inevitably several networks will form. It was found that networks will often divide into smaller networks or join together into larger networks. Each scenario was run ten times with a different seed value for the PRNG, resulting in a very different network formation, and the results averaged. This was useful for comparison as after each series of ten simulations, the seed values were used for the following ten with variables changed. This meant the simulation runs appeared identical at the beginning of the simulations with node placement and mobility and assisted with identifying trends caused by the altered variables.

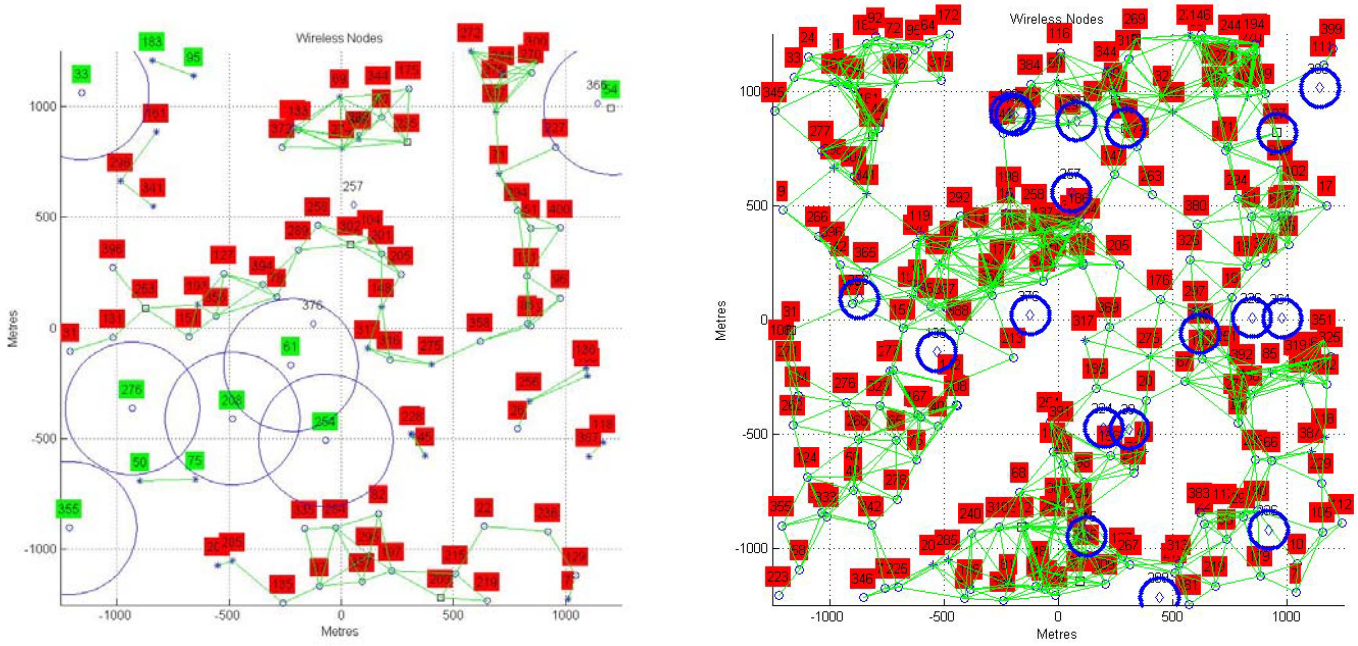

Figure 1: Simulation snapshot at 200 seconds and 600seconds

Figure 1 left shows the network scenario generated after 200 seconds of simulation time forming 8 networks. The nodes with a large circle around them (representing 300 metres) are out of range of another node, with darker node markers indicating nodes currently holding PKI certificates. Node 257 in the middle just above half way (represented by a diamond) has been ejected from the network. Figure 1 right shows the same simulation after the full 600 seconds and ends with a single large network. The smaller circles around the diamonds show the 18 malicious nodes that have been ejected. Results were collected for certificate success and the parameters altered to view the change in success of those requests. Degradation in performance was not significant until a threshold of 5 servers and a trust threshold value of 0.6. Any more than 5 servers proved impractical and raising the trust threshold along the certificate chain above 0.6 also degraded performance to an unacceptable level. Security within networks could be increased, either by requiring a higher threshold of trust for the certificate request message, or by requiring more servers to be contacted to receive a certificate, or a combination of both. Forensic evidence was bound to the certificate management and dynamically logged.

DISCUSSION

Mobility has shown to make a slight difference in increasing certificate request success. However, malicious behaviour has shown a significant effect in certificate request failures resulting in a node making more than one request for a certificate. Therefore, the ability of this protocol to handle mobile nodes and to identify

misbehaving nodes and then permanently eject them is a desirable feature helping to stabilise the network and maintain robustness against misbehaving nodes.

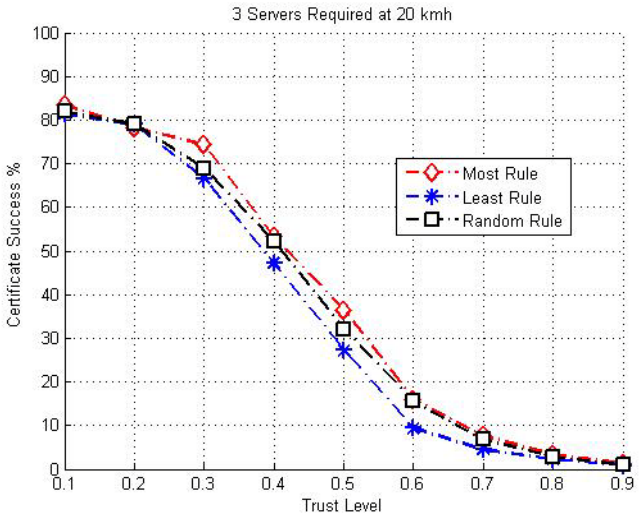

Figure 2: 3 servers required with 20% mobility at 20-29kmh

Figure 2 shows that when 3 servers are required for a certificate, the placement of the servers has a noticeable impact on the efficiency of the protocol. In the middle range the effect is most noticeable. Here, nodes with the most number of neighbours taking on a server role proved to be the most effective. Conversely, those with the least number of neighbours proved to be the worst choice. This is because nodes placed nearer the centre of the network, on average, required fewer hops to reach. Additionally, if all servers were located near the centre of the network, then they tended to be close together. This made inter-server communication very efficient, and as the server threshold was increased the inter-server closeness made certificate issuance more and more efficient. The distance to the first server became less important than the distance from first server to the other servers. Having to inform new nodes of the number of servers in the network creates more management messages using up valuable network time. However, for more than two servers required, the extra overhead of this 'informed' proved warranted. As the required trust calculation made by the server for a certificate request is raised, the percentage of certificates refused increases. Additionally, requiring more servers to be contacted requires a longer certificate chain. An increase in the length of the certificate chain (hops) increases the likelihood of the chain encountering a malicious node and therefore a failure.

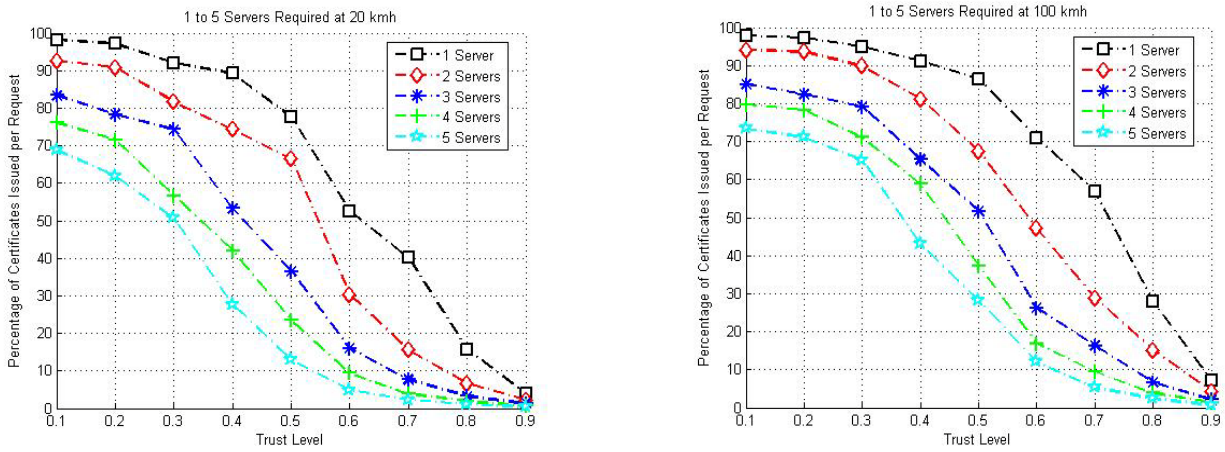

Figure 3: 1-5 servers required with 20% mobile at 20kmh and100kmh

These results show that as the nodes in the network increase in speed, the successful certificate issuance ratio increases. This is because the routes to the servers change fairly rapidly meaning a refused initial request will

result in a re-request likely taking a different path to a server and therefore having a renewed chance of success. Figure 3 left shows 20% of nodes mobile at relatively slow speeds. This could represent slow driving or perhaps boats navigating a flooded area. The mobility of even a small percentage of nodes results in an increase in certificate issuance success, especially in the mid trust thresholds of 0.3 - 0.8. The trust threshold ensures increased security but at the cost of requests more likely to fail as hop counts for certificates increases. As speeds of mobile nodes increases, the mobility of nodes further assists in this scenario as nodes and servers may move closer to each other reducing the number of hops required and increasing the chance of success with each retry. The hops for a successful certificate request necessarily reduce as very long hops will almost always result in a refusal. Here, the informed requests results in considerably fewer requests and much shorter hops to receive the certificate. The optimum trust level was found to be in the region of 0.4 to 0.5. Therefore, the security level required for the network should be considered carefully as increasing security of key management system services by increasing the trust threshold has a severe impact on message passing performance.

CONCLUSION

SKYE works well within the limitations set by entirely online network formation and key management. The simulator shows that the performance of SKYE is realistic. Further changes to both the protocol and to the simulator are planned to include evidential retention rules in addition to the current issue and revocation logs. Firstly, the server rules will be enhanced so that groups of servers will be located using the current server rules. For example, if 5 servers are required, then up to 5 servers will be located as neighbours and the group of servers will be located according to the current rules, rather than an individual server. The simulator would benefit from implementing such attributes as signal attenuation, bit error rates and at least one fully functional routing algorithm. This would enhance the simulator's realism to where it could be used for the complete security forensic scenario.

REFERENCES

Capkun, S. Buttyan, L. and Hubaux, J.P. (2003). Self-Organized Public-Key Management for Mobile Ad Hoc Networks. *IEEE Transactions on Mobile Computing*, 2(1): p. 52-64.

Chen, G., Yao, H. and Wang, Z. (2010). An intelligent WLAN intrusion prevention system based on signature and plan recognition. Proceedings of the Second International Conference on Future Networks, pp. 168-172.

Frankel, S., Eydt, B, Owens, L. and Scarefone, K. (2007). Special Publication 800-97: Establishing wireless robust security networks: A guide to IEEE 802.11i. NIST: Maryland.

Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T. (2007). Secure Distributed Key Generation for Discrete-Log Based Cryptosystems. *J. Cryptology* 51-83

Hyytiä, E. and Virtamo, J. (2007). Random Waypoint Mobility Model in Cellular Networks, *Wireless Networks*, 13(2): p.177-188.

Johnson, D. B. and Maltz, D. A. (1996). Dynamic Source Routing in Ad Hoc Wireless Networks. in Imielinski and Korth, (Eds.). *Mobile Computing.* vol. 353. Kluwer Academic Publishers.

Kong, J. Zerfos, P. Luo, H. Lu, S. and Zhang, L. (2001). Providing Robust and Ubiquitous Security Support for Mobile Ad-hoc Networks. in *Ninth International Conference on Network Protocols ICNP2001*

Kurkowski, S. Camp, T. and Colagrosso, M. (2005). MANET simulation studies: the incredibles. *SIGMOBILE Mob. Comput. Commun. Rev.*, 9(4): p. 50-61.

New Zealand Police. (2004). "New Zealand Crime Statistics". Retrieved 15th January 2010 from http://www.justice.govt.nz/publications/global-publications/r/research-on-the-effectiveness-of-police-practice-in-reducing-residential-burglary-november-2005-report-7-case-study-of-the-sydenham-police-area/10-crime-statistics.

Yi, S. and Kravets, R.(2003). MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks. *Annual PKI Research Workshop Program*. Maryland, USA.

Yi, S. and Kravets. R. (2004). Composite Key Management for Ad Hoc Networks. In *The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services MOBIQUITOUS 2004.*

Zhou, L. and Haas, Z. (1999). Securing Ad Hoc Networks. *IEEE Network*, 13(6): 24-30.

Zhu, B. Bao, F. Deng , R. H. Kankanhalli M. S. and Wang , G. (2005). Efficient and Robust Key Management for Large Mobile Ad hoc Networks. Computer Networks, 2005. 48(4): p. 657-682.

Zimmerman, P. (1994). *PGP User's Guide*. Cambridge MA: MIT.

Wu, B. Wu, J. Fernandez, E. B. Ilyas, M. and Magliveras, S. (2005). Secure and Efficient Key Management in Mobile Ad Hoc Networks, *Journal of Network and Computer Applications (JNCA)*, Vol. 30, 937–954